



⑮ **BUNDESREPUBLIK
DEUTSCHLAND**



**DEUTSCHES
PATENT- UND
MARKENAMT**

⑫ **Offenlegungsschrift**
⑩ **DE 198 20 605 A 1**

⑤① Int. Cl.⁶:
G 06 F 17/60

⑲ Aktenzeichen: 198 20 605.4
⑳ Anmeldetag: 8. 5. 98
㉑ Offenlegungstag: 11. 11. 99

DE 198 20 605 A 1

⑦① Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

⑦② Erfinder:
Seysen, Martin, Dr., 80809 München, DE

⑤⑤ Für die Beurteilung der Patentfähigkeit in Betracht
zu ziehende Druckschriften:

DE	36 19 566 C2
DE	38 22 540 A1
DE	695 00 523 T2
US	55 13 133
US	52 99 263
EP	05 78 059 A1
EP	05 77 000 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

⑤④ Verfahren zur sicheren Verteilung von Software

⑤⑦ Die Erfindung betrifft ein Verfahren zur sicheren Verteilung von Daten und/oder Programmen, wobei die zu übertragenden Daten mit einer elektronischen Unterschrift versehen werden. Diese elektronische Unterschrift wird in der die Daten und/oder Programme enthaltenden Stelle überprüft, indem eine modulare Multiplikation ausgeführt wird, wozu eine Multiplikation und eine Division erforderlich ist. Gemäß der Erfindung wird zur Überprüfung der Unterschrift in der die Daten und/oder Programme erhaltenen Stelle eine modulare Multiplikation nach Montgomery durchgeführt, bei der eine zusätzliche Multiplikation mit einem Faktor auf der Grundlage der Basis 2 und geradzahligen Exponenten durchgeführt wird.

DE 198 20 605 A 1

Die Erfindung betrifft ein Verfahren zur sicheren Verteilung von Daten und/oder Programmen nach dem Oberbegriff des Anspruchs 1.

Verfahren zur Verteilung von Software SW von einer ausgeben- 5 den Stelle an eine große Anzahl von gleichartigen Terminals bzw. an Chipkarten finden insbesondere durch die Möglichkeiten der Datenfernübertragung immer mehr Verwendung. Die ausgebende Stelle erzeugt eine elektronische Unterschrift der Software SW mit Hilfe eines Public-Key Verfahrens, um die Authentizität der Software SW sicherzu- 10 stellen.

Dafür berechnet die herausgebende Stelle nach einem allgemein bekannten Verfahren ein Zertifikat M der zu unterschreibenden Software SW, welches neben anderen Daten vor allem einen von der Software abhängigen Hash-Wert $H(SW)$ enthält. Hierbei ist $H(SW)$ ein öffentlich bekanntes Hash-Verfahren. Die herausgebende Stelle verschlüsselt das Zertifikat M mit ihrem privaten Schlüssel D. Das Ergebnis dieser Verschlüsselung ist die elektronische Unterschrift S. Die herausgebende Stelle sendet die Software SW zusammen mit der Unterschrift S an das Terminal oder die Chipkarte. Dort wird aus der Unterschrift S mit Hilfe des öffentlichen Schlüssels $E = D^{-1}$ der herausgebenden Stelle der Wert M des erzeugten Zertifikates berechnet. Ferner berechnet das Terminal bzw. die Chipkarte, d. h. die empfangende Stelle den Hash-Wert $H(SW)$ der Software SW und prüft, ob $H(SW)$ in dem Zertifikat M korrekt eingetragen ist. Wenn dies der Fall ist, akzeptiert die empfangende Stelle die Software SW, andernfalls weist sie die Software SW zurück.

Das bekannteste Public-Key Verfahren zur Erzeugung von elektronischen Unterschriften ist das RSA-Verfahren. Eine Variante des RSA-Verfahrens ist das Verfahren von Rabin oder eine Variante des Rabin-Verfahrens nach Williams. 35

Die ausgebende Stelle wählt zufällig zwei Primzahlen $P = 3 \bmod 8$ und $Q = 7 \bmod 8$. Diese stellen den privaten Schlüssel von der ausgebenden Stelle dar. Der öffentliche Schlüssel ist der Wert $N = P \cdot Q$. Zum Unterschreiben einer Nachricht M berechnet die ausgebende Stelle die Unterschrift

$$S = M^{1/2} \bmod (P \cdot Q).$$

Die empfangende Stelle kann die Unterschrift verifizieren, indem sie

$$M = S^2 \bmod N$$

berechnet.

Die Sicherheit des Rabin-Verfahrens beruht darauf, daß das Ziehen der Quadratwurzel einer Zahl modulo einer Primzahl (falls eine solche existiert) einfach ist, während das Ziehen der Quadratwurzel einer zufällig gewählten Zahl modulo einer zusammengesetzten Zahl mindestens ebenso schwierig ist die Faktorisierung jener zusammengesetzten Zahl.

Nicht jede Zahl ist quadratischer Rest modulo einer Primzahl P oder Q; außerdem haben quadratische Reste mod P und Q in der Regel vier Quadratwurzeln. Aufgrund der speziellen Wahl von P und Q ist für jede beliebige Zahl M genau eine der vier Zahlen M, N-M, N/2 und N-M/2 quadratischer Rest mod P und mod Q (Bei ungeradem M wird N/2 durch $(M+N)/2 \bmod P \cdot Q$ ersetzt). Diese Aussage folgt aus den Ergänzungssätzen zum quadratischen Reziprozitätsgesetz.

Fordert man für die Nachricht M die zusätzliche Bedingung $M = 4 \bmod 8$, so gilt wegen der Beziehung $N = P \cdot Q = 3 \cdot 7 = 5 \bmod 8$ folgendes:

$$M = 0, N-M = 1, M/2 = 2, M-N/2 = 3 \bmod 4$$

d. h. die vier Zahlen M, N-M, M/2 und N-M/2 unterscheiden sich in den letzten beiden Binärstellen.

Zum Unterschreiben einer Nachricht M prüft die ausgebende Stelle zunächst, welcher der vier Werte M, N-M, N/2 oder N-N/2 quadratischer Rest mod P und mod Q ist. Dies kann effektiv durch Berechnen der Jacobi-Symbole (N/P) und (M/Q) erfolgen:

$$M' = M \text{ falls } (M/P) = 1, (M/Q) = 1;$$

$$M' = -M \text{ falls } (M/P) = -1, (M/Q) = -1;$$

$$M' = M/2 \text{ falls } (M/P) = -1, (M/Q) = 1;$$

$$M' = -M/2 \text{ falls } (M/P) = 1, (M/Q) = -1.$$

Sei M' derjenige Wert, der beide Bedingungen erfüllt. Die Unterschrift zu der Nachricht M ist dann:

$$S = (M')^{(P-1)/2 \cdot (Q-1)/2} \bmod N.$$

Es gilt also:

$$S^2 = M' \cdot (M')^{[(P-1)/2] \cdot [(Q-1)/2]} \bmod N.$$

Da M' quadratischer Rest mod P ist, folgt nach dem kleinen Fermat'schen Satz $(M')^{(P-1)/2} = 1 \bmod P$. Analog gilt $(M')^{[(Q-1)/2]} = 1 \bmod Q$. Nach dem chinesischen Restsatz folgt weiter $(M')^{[(P-1)/2] \cdot [(Q-1)/2]} = 1 \bmod P \cdot Q$. Es gilt also

$$S^2 = M' \bmod N = P \cdot Q.$$

Zum Verifizieren der Unterschrift S berechnet das Terminal B zunächst den Wert

$$M' = S^2 \bmod N.$$

Da sich bei gegebenem $M = 4 \bmod 8$ die vier möglichen Werte für M in den letzten beiden Binärstellen unterscheiden, läßt sich M leicht aus M' berechnen:

$$M = M' \text{ falls } M' = 0 \bmod 4;$$

$$M = N-M' \text{ falls } M' = 1 \bmod 4;$$

$$M = 2M' \text{ falls } M' = 2 \bmod 4;$$

$$M = 2(N-M') \text{ falls } M' = 3 \bmod 4.$$

Zum Verifizieren einer Unterschrift auf der Chipkarte oder dem Terminal B ist eine modulare Multiplikation erforderlich; d. h. die empfangende Stelle berechnet:

$$M' = S \cdot S \bmod N.$$

Hierzu ist eine Multiplikation und eine Division erforderlich. Dabei ist die Division um einiges aufwendiger als die Multiplikation. Der Nachteil der bekannten Verfahrensweise zum Verifizieren einer Unterschrift besteht also darin, daß bei der die Software empfangenden Stelle, die üblicherweise weniger Rechenkapazität zur Verfügung hat als die ausgebende Stelle, eine vergleichsweise aufwendige Rechenoperation durchführen muß.

Es ist deshalb Aufgabe der Erfindung, ein Verfahren zum sicheren Verteilen von Software anzugeben, bei dem obige Nachteile vermieden werden.

Ausgehend von den Merkmalen des Oberbegriffs des Anspruchs 1 wird diese Aufgabe durch die kennzeichnenden Merkmale des Anspruchs 1 gelöst.

Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Gemäß der Erfindung wird anstelle der üblichen Standardverfahren für Langzahlarithmetik (Trial Division) ein Verfahren nach Montgomery für die Verifizierung der elektronischen Unterschrift eingesetzt. Montgomery beschreibt

ein schnelleres Verfahren zur modularen Multiplikation, welches statt des Produktes $Z = X \cdot Y$ modulo N den folgenden Wert berechnet:

$$Z0 = X \cdot Y \cdot L^{-i} \bmod N.$$

Hierbei ist L die Basis, bezüglich welcher die Langzahlarithmetik durchgeführt wird. Typischerweise wird $L = 2^8$ bei einem 8-Bit Prozessor verwendet, $L = 2^{16}$ bei einem 16-Bit Prozessor, usw. gewählt. Der Wert i muß mindestens so groß sein, daß die Bedingung

$$L^i > N$$

erfüllt ist.

Der Vorteil des Montgomery-Verfahrens besteht darin, daß der Schritt der "Trial-Division" bei der modularen Multiplikation entfällt. Dafür wird zusätzlich mit dem unerwünschten Faktor $L^{-i} \bmod N$ multipliziert. Die Kompensation dieses unerwünschten Effektes bei der modularen Exponentiation nach dem RSA-Verfahren kann wie folgt geschehen:

Die Berechnung einer RSA-Exponentiation $A^E \bmod N$ wird üblicherweise durch wiederholte Anwendung der Potenzgesetze $A^{2x} = A^x \cdot A^x \bmod N$ und $A^{2x+1} = (A^x \cdot A^x) \cdot A \bmod N$ durchgeführt. Im ersten Schritt wird $X = (E/2)$ gesetzt, und in den Folgeschritten wird X solange durch $(X/2)$ ersetzt bis $X = 1$ gilt; hierbei ist (X) die größte ganze Zahl $\leq X$. Faktisch wird die modulare Exponentiation damit auf eine Folge von Quadrierungen und Multiplikationen mit der Basis $A \bmod N$ zurückgeführt.

Bei der modularen Exponentiation mit dem Montgomery-Verfahren wird folgendes berechnet:

$$A0 = (A0 \cdot (L^{2i} \bmod N)) \cdot L^i \bmod N.$$

Diese erfordert eine Montgomery-Multiplikation mit dem festen Wert $L^{2i} \bmod N$ und es gilt $A0 = A \cdot L^i \bmod N$. Offensichtlich gilt:

$$A^x \cdot A^y \cdot L^i = (A^x \cdot L^i) \cdot (A^y \cdot L^i) \cdot L^i = A^{x+y} \cdot L^i \bmod N.$$

Mit Hilfe von $(A^x \cdot L^i)$ und $(A^y \cdot L^i)$ läßt sich also der Wert $A^x \cdot A^y \cdot L^i$ durch eine einzige Montgomery-Multiplikation berechnen. Beginnend mit dem Wert $A0 = A \cdot L^i$ läßt sich durch wiederholtes Quadrieren und Multiplizieren mit $A0$ leicht der Wert $A^E \cdot L^i$ berechnen. Eine weitere Montgomery Multiplikation des Zwischenergebnisses $A^E \cdot L^i$ mit 1 liefert das gewünschte Endergebnis A^E .

Bei der modularen Exponentiation mit einem zufällig im Bereich $1, \dots, N$ gewählten Exponenten entsteht durch eine erforderliche Kompensation ein relativ geringer zusätzlicher Rechenaufwand.

Bei einem Software-Download in ein Terminal oder eine Chipkarte muß dort die Unterschriftsprüfung durchgeführt werden. Da das Terminal in der Regel über wenig Rechenleistung verfügt, muß die Unterschriftsprüfung so einfach wie möglich realisiert werden.

Bei der herkömmlichen Kombination der Unterschriftsprüfung nach Rabin mit der Montgomery-Multiplikation wird die Unterschrift S an das Terminal B übertragen.

Das Terminal B berechnet:

$$M0 = (S \cdot S) \cdot L^{-i} \bmod N$$

$$M' = (M0 \cdot (L^{2i} \bmod N)) L^{-i} \bmod N.$$

Offensichtlich gilt dann $M' = S^2 \bmod N$. Dieses Verfahren erfordert zwei Montgomery-Multiplikationen mod N und es

muß außerdem der Wert $(L^{2i} \bmod N)$ in der empfangenden Stelle gespeichert werden.

Gemäß einer vorteilhaften Ausgestaltung der Erfindung, wird deshalb folgende Modifikation vorgenommen, welche gegenüber dem herkömmlichen Verfahren eine Montgomery-Multiplikation und das Speichern des Wertes $(L^{2i} \bmod N)$ nicht benötigt. Anstelle der Unterschrift S wird die modifizierte Unterschrift

$$S' = S \cdot L^{i/2} \bmod N$$

an die empfangende Stelle übertragen. Da L bei handelsüblichen Prozessoren eine gerade Zweierpotenz ist, läßt sich $L^{i/2}$ leicht berechnen. Die empfangende Stelle berechnet nun nach dem Montgomery-Verfahren den Wert

$$(S' \cdot S') \cdot L^{-i} \bmod N = (S \cdot L^{i/2} \cdot S \cdot L^{i/2}) L^{-i} \bmod N = S^2 \bmod N = M' \bmod N.$$

Somit erfordert die Unterschriftsprüfung nur eine Montgomery-Multiplikation auf dem Terminal.

Patentansprüche

1. Verfahren zur sicheren Verteilung von Daten und/oder Programmen, wobei die zu übertragenden Daten mit einer elektronischen Unterschrift, vorzugsweise nach einem Public-Key-Verfahren erzeugt, versehen werden, wobei diese elektronische Unterschrift in der die Daten und/oder Programme erhaltenen Stelle überprüft wird und zur Überprüfung eine modulare Multiplikation ausgeführt wird, wozu eine Multiplikation und eine Division erforderlich ist, **dadurch gekennzeichnet**, daß zur Überprüfung der Unterschrift in der die Daten und/oder Programme erhaltenen Stelle der Überprüfung der Unterschrift eine modulare Multiplikation nach Montgomery durchführt, bei der eine zusätzliche Multiplikation mit einem Faktor auf Grundlage der Basis 2 und geradzahlgigen Exponenten durchgeführt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß in der die Daten und/oder Programme ausgebenen Stelle die digitale Unterschrift mit einem aus der Montgomery-Multiplikation abgeleiteten Faktor multipliziert wird, so daß sich auf der die Daten und/oder Programme erhaltenen Stelle der zusätzliche Multiplikationsfaktor herauskürzt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Daten und/oder Programme zu einem Chip-Karten-Terminal oder einer Chipkarte übertragen werden.

- Leerseite -